UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,170	03/06/2002	John G. Kennedy	5681-10100	9235

7590 09/08/2006

Robert C. Kowert
Conley, Ross, & Tayon, P.C.
P.O. Box 398
Austin, TX 78767

EXAMINER	
HOSSAIN, TANIM M	
ART UNIT	**PAPER NUMBER**
2145	

DATE MAILED: 09/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

SEP 0 8 2006

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/092,170
Filing Date: March 06, 2002
Appellant(s): KENNEDY, JOHN G.

Robert C. Kowert
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed May 30, 2006 appealing from the Office action mailed February 1, 2006.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0019870	Chirashnya, et al.	2/2002
2003/0048782	Rogers, et al.	3/2003
2003/0051049	Noy, et al.	3/2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-15, 22-31, and 33-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Chirashnya (U.S. 2002/0019870).

As per claim 1, Chirashnya teaches a system comprising: a network system comprising a plurality of network components (paragraph 0001); a host computer system coupled to the network system, wherein the host computer system is configured to: perform system discovery to generate data indicative of a configuration of the plurality of network components (0003); detect a failure of one of the components included in the plurality of network components (0015); in response to identifying the failed component, update an availability of the network system using the data indicative of the configuration of the plurality of network components (0034, 0047, 0048, 0051, 0059); and store data indicative of the availability of the network system (0019).

As per claim 2, Chirashnya teaches the system of claim 1, wherein the host computer system is configured to use the updated availability to calculate a risk of the network system becoming unavailable during one or more exposure periods following the failure and prior to a repair or replacement of the failed component, and store data indicative of the risk (0024, 0035).

As per claim 3, Chirashnya teaches the system of claim 2, wherein the data indicative of a risk includes data indicative of a probability of the network system becoming unavailable during each of the one or more exposure periods (0010).

As per claim 4, Chirashnya teaches the system of claim 2, wherein the data indicative of the risk includes data indicative of an expected number of system failures per a given population for each of the one or more exposure periods (0026).

As per claim 5, Chirashnya teaches the system of claim 2, wherein the host computer system is configured to compare the risk of the network system becoming unavailable for a first exposure period of the one or more exposure periods to a threshold value (0020, 0022, 0027, 0063); and if the risk is higher than the threshold value, determine an acceptable exposure period, wherein the risk of the network system becoming unavailable during the acceptable exposure period is lower than the threshold value, and provide an indication of the acceptable exposure period (0054, 0063).

As per claim 6, Chirashnya teaches the system of claim 1, wherein the host computer system is configured to update the availability of the network system by calculating the instantaneous availability of the plurality of network components by calculating the instantaneous availability of the plurality of network components (0011, 0048).

As per claim 7, Chirashnya teaches a computer readable medium comprising program instructions computer executable to: receive data indicating a configuration of components included in a network system; receive an indication of a failure of one of the components in the network system; compute an availability of the network system from the data in response to the failure of one of the components, and store availability data comprising data indicative of the availability of the network system (0003, 0005, 0019, 0030, 0034, 0047, 0048, 0051, 0059).

As per claim 8, Chirashnya teaches the computer readable medium of claim 7, wherein the availability data comprises a table comprising one or more entries, wherein each entry in the

table indicates a risk of the network system being disrupted during a respective exposure period, following the failure and prior to a repair or replacement of the failed component, wherein the risk depends on the availability of the network system (0019, 0033, 0050).

As per claim 9, Chirashnya teaches the computer readable medium of claim 8, wherein each entry in the table indicates a probability of the network system being disrupted during the respective exposure period (0033).

As per claim 10, Chirashnya teaches the computer readable medium of claim 8, wherein each entry in the table indicates an expected number of system failures per a given population for the respective exposure period (0026).

As per claim 11, Chirashnya teaches the computer readable medium of claim 8, wherein a first exposure time of the one or more exposure period is an estimated period to replace the one of the components that failed (0054).

As per claim 12, Chirashnya teaches the computer readable medium of claim 7, wherein the program instructions are computer executable to evaluate the risk of the network system being disrupted by comparing the risk of the network system being disrupted for at least one of the one or more exposure periods to a threshold risk (0047, 0063).

As per claim 13, Chirashnya teaches the computer readable medium of claim 12, wherein the program instructions are computer executable to store an indication of an unacceptably high risk in response to the risk of the network system being disrupted for at least one of the one or more time periods being greater than the threshold risk (0048).

As per claim 14, Chirashnya teaches the computer readable medium of claim 13, wherein the indication of the unacceptably high risk includes an indication of an acceptable exposure period (0054).

As per claim 15, Chirashnya teaches the computer readable medium of claim 14, wherein the program instructions are computer executable to provide the acceptable exposure period to a monitoring device (0059).

As per claim 22, Chirashnya teaches the computer readable medium of claim 7, wherein the program instructions are computer executable to compute the availability of the network system by computing the instantaneous availability of the network system (0010).

Claims 23, 24, 25, 26, 27, 28, 29, and 30 are rejected on the same bases as claims 1, 2, 3, 4, 5, 13, 14, and 15 respectively.

As per claim 31, Chirashnya teaches the method of claim 24, wherein a first exposure time of the one or more exposure times is an estimated time to replace the one of the components that failed (0054).

As per claim 33, Chirashnya teaches the method of claim 23, wherein said computing comprises calculating the instantaneous availability of the network system (0011).

As per claim 34, Chirashnya teaches a system comprising: a network system comprising a plurality of components; means for performing system discovery for the network system, wherein the means for performing system discovery generate data indicative of a configuration of the network system; means for detecting a failure of one of the plurality of network components; and means for calculating an availability of the network system from the data generated by the means for performing system discovery, wherein the means for calculating an

availability calculate the availability in response to the means for detecting a failure detecting that a first one of the plurality of network components ha failed, wherein the means for calculating the availability store data indicative of the availability of the network system (0011, 0054, 0019, 0033, 0050).

Claim 35 is rejected on the same basis as claim 34.

As per claim 36, Chirashnya teaches the system of claim 35, wherein the first network device is a host computer system (0006).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 16-19, 32, 37, 38, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chirashnya (U.S. 2002/0019870).

As per claims 16-19, Chirashnya teaches the system of claim 7, but does not specifically teach the use of block diagram analysis, fault tree analysis, Markov chain analysis, and Monte Carlo analysis. These types of analyses are merely different statistical risk analyses. It would have been obvious to one of ordinary skill in the art at the time of the invention to include these various types of analysis. Chirashnya chooses to use a Bayesian analysis, and therefore differing

analyses constitute a design choice rather than a patentable distinction, because one of ordinary skill in the art at the time of the invention would have known to use whichever types of probability analyses as he/she sees fit.

Claim 32 is rejected on the same basis as claim 16.

As per claims 37 and 38, Chirashnya teaches the system of claim 35, but does not specifically teach that the network device is an array controller or network switch. It would have been obvious to one of ordinary skill in the art at the time of the invention to include specifically these network components. The motivation for doing so lies in the fact that either of these components have the ability to monitor and control the network for functionality probabilities. Chirashnya does not limit the use of any network component, which would render the inclusion of an array controller or network switch abundantly obvious to one of ordinary skill in the art at the time of the invention.

As per claim 40, Chirashnya teaches the system of claim 1, wherein said detecting the failure comprises: monitoring performance of one of the components (0009), but does not specifically teach the determination that a component has failed if its performance falls below a threshold. Official notice is taken that the inclusion of a threshold value to determine component failure is well known in the art, wherever network performance is being monitored. It would have been obvious to one of ordinary skill in the art at the time of the invention to include the well-known component of a failure threshold to determine whether or not the component is failing.

Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chirashnya in view of Rogers (U.S. 2003/0048782).

As per claim 20, Chirashnya teaches the system of claim 7, but does not specifically teach the calculation of non-redundant components by multiplying probabilities. Rogers teaches the calculation of independent non-redundant components' availabilities by multiplication (page 1). It would have been obvious to one of ordinary skill in the art at the time of the invention to include the independent calculation of non-redundant components as taught by Rogers in the system of Chirashnya. The motivation for doing do lies in the fact that having an additional method of probability calculation would lend itself to a more robust invention, capable of handling multiple calculations, leading to additional analysis. Both inventions are from the same field of endeavor, namely the probabilistic monitoring of computer networks.

As per claim 21, Chirashnya-Rogers teaches computer readable medium of claim 20, wherein at least one of the non-redundant components includes a plurality of redundant components (page 1).

Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chirashnya in view of Noy (U.S. 2003/0051049).

As per claim 39, Chirashnya teaches the system of claim 1, but does not specifically teach that the system discovery entails a sending a request for identification of the network component, and returning an identifier in response. Noy teaches the unique identification of a network component by request (0008). It would have been obvious to one of ordinary skill in the art at the time of the invention to include the specific identification of a network component

through system discovery, as taught by Noy in the system of Chirashnya. The motivation for doing so lies in the fact that identification of the components would enable more efficient monitoring of the components, which would facilitate response in case of a failure. Both inventions are from the same field of endeavor, namely the monitoring of network components.

(10) Response to Argument

Claims 1, 7, 23, 34, 35, and 36:

Appellant states that "in regard to claim 1, Chirashnya does not teach updating an availability of a network system in response to identifying a failed component, nor does Chirashnya teach using configuration data obtained via system discovery to update the availability of the network system." Examiner respectfully disagrees. Appellant's citations of paragraphs 0052 and 0059, in terms of comparing malfunction rates to baseline values only highlights an additional feature in Chirashnya's invention, and not the invention as a whole.

In paragraph 0010, Chirashnya discusses the maintenance of up-to-date topology information regarding the network as a whole, which constitutes the updating of an availability. Further, paragraph 0010 teaches the receiving of an alarm (corresponding to a fault), which results in the building of a Bayesian network, where updated failure rates are calculated based on this. This also constitutes the availability of a network in response to identifying a failed component – the system updates continuously to reflect the most recent values and configuration.

The fault affects the system as a whole, and as such, probabilities are calculated as a whole, which is the basis of Bayesian conditional probability.

Paragraph 0011 states that "these models completely and accurately reflect the actual, current network conditions..."

Paragraphs 0019 and 0033 state that the latest network configurations are stored in a database, such that they may be used to construct the causal network. This constitutes using configuration data obtained via system discovery to update the availability of the network system.

Paragraph 0023 discusses the probabilities of other modules failing, in response to a fault in a certain module. These probabilities are updated upon its occurrence, further constituting the claimed elements.

Paragraph 0047 and 0048 discuss the monitoring of the network for devices not responding, statistics that may reflect abnormal functionality, and configuration changes. This teaching further constitutes performing system discovery to generate data indicative of a configuration of the plurality of network.

Paragraphs 0051 and 0052 disclose the database tracking and containing the complete configuration of the network. The database is then "updated automatically, in real time, to reflect any changes that occur, such as addition or removal of nodes." In response to alarms, reliability assessments take place, and the calculation of the malfunction rate of each module takes place. This clearly constitutes the updating of the availability in response to a failure, and storage of data indicative of the availability of the network system.

Paragraphs 0061 and 0062 further teach the updating of an availability of the network in response to a failed component, using the data indicative of the configuration of the plurality of network components.

In view of the above-mentioned disclosures and suggestions, Chirashnya clearly teaches each limitation as claimed.

Claims 2, 8, and 24:

Appellant asserts that Chirashnya does not teach using the updated availability to calculate a risk of the network system becoming unavailable during one or more exposure periods following the failure and prior to a repair or replacement of the failed component, and storing data indicative of the risk. Examiner respectfully disagrees.

As a singular example, paragraph 0054 of Chirashnya discusses the obtaining of malfunction probabilities, which may be presented in a variety of ways, such as with an MTBF measurement, accompanied by a measure of confidence in the estimate. In the disclosure, as discussed above, the availability is continually updating, and with it are the malfunction rates of the modules (see paragraph 0062 as another example). As such, MTBF measurements and their related confidences constitute the risk of the network system becoming unavailable. Because Chirashnya's system is updating continually, the risk is being calculated upon the initialization of the network, after an alarm sounds (which follows the failure and is before the repair of the failed component), and after this component is replaced, for example. Paragraph 0062 discusses updating the probability tables of the nodes based on the alarms, which then constitutes the

storing of data indicative of the risk. As such, the claims in question are fully disclosed in Chirashnya.

Claims 3, 9, and 25:

Appellant asserts that Chirashnya does not teach that the data indicative of the risk includes data indicative of a probability of the network system becoming unavailable during each of the one or more exposure periods.

As discussed above, Chirashnya teaches the updating of failure probabilities of network components (paragraphs 0047, 0054, 0062, among others). If these components fail, an alarm is sounded, and the components become unavailable, which is then updated in the database of configuration information. The causal network also reflects this change in its probabilities of failure. Because the risk deals in malfunction rates, it indicates the probability that the network system may become unavailable.

Claims 4, 10, and 26:

Chirashnya teaches that the data indicative of the risk includes data indicative of an expected number of system failures per a given population for each of the one or more exposure periods.

In paragraphs 0053 and 0054, Chirashnya teaches global fault information, where the distribution of expected rates of failure are used. As such, the probability of system failures per

a given population (global, in this case) is constituted. The use of MTBF (Mean Time Between Failures) in conjunction with a confidence related to it is indicative of an expected number of failures, where a high confidence in a given MTBF value is indicative of a higher probability of that system component failing at a given time. Based on the time period between the alarm occurring, and an action taking place (the claimed exposure period), the MTBF falling within the exposure period and its related confidence probability would be used to arrive at the number of expected failures during that exposure period. Therefore, data indicative of an expected number of system failures is disclosed, and Chirashnya teaches the claims in question.

Claims 5, 6, 11, 12, 13, 14, 15, 27, 28, 29, 30, and 31:

As per the discussion of claim 5, Chirashnya teaches the determination of an acceptable exposure period, wherein the risk of the network system becoming unavailable during the acceptable exposure period is lower than the threshold value, and the providing of an indication of the acceptable exposure threshold.

In paragraphs 0053, 0054, and 0063, Chirashnya discusses an MTBF, and a confidence probability related to it. If the actual MTBF drops below the MTBF threshold (10^8, in this example) with more than a 10% confidence, the module is flagged. As such, the acceptable exposure period is simply the MTBF. The confidence percentage governs the risk that the module may drop below that acceptable MTBF. Therefore, Chirashnya discloses claim 5.

The disclosure of claim 6 is discussed above, and given that the causal network continually updates, an instantaneous availability is constituted.

As per claims 11 and 31, the MTBF after an alarm indicates the amount of time available to replace that component before it fails, which constitutes an estimated time to replace the failed components (see paragraph 0063).

As per claims 12, 13, 14, 15, 27, 28, 29, and 30 as discussed earlier, Chirashnya discusses evaluating the risk, such that the MTBF falls below a threshold, with a confidence probability associated with it. If the confidence probability of the MTBF reaches a level higher than the set threshold, the component is flagged (it has an unacceptably high risk). The probabilities and parameters continually change during the exposure periods, and are thus clearly stored for the system to have functionality (0053, 0054, 0063). The system as a whole provides a monitoring service, where the MTBF is held as a threshold value, below which the actual value may not drop (above a certain confidence level). Because action is taken if this happens, the provision of the acceptable exposure period to a monitoring service takes place. Please also see the discussion of claim 5.

Claims 16-19, 32, 37, and 38:

Chirashnya teaches the use of Bayesian analyses and Poisson analyses to calculate the availability of the network. It can reasonably be assumed that one of ordinary skill in the art at the time of the invention would have thought to use other forms of statistical analyses to put the invention into practice. Because reliability block, fault tree, Monte Carlo, and Markov chain analyses are other types of statistical analyses, it would have been obvious to one of ordinary

skill in the art to employ these analyses at the time of the invention, in view of Chirashnya's use of the Bayesian and Poisson analyses.

Claims 20, 21, 22, and 33:

Claim 20 discloses the multiplication of individual availabilities of each non-redundant component to arrive at a calculation of the availability of the group of non-redundant components. This is the concept of arriving at a probability of independent events. Rogers teaches the multiplication of individual probabilities to arrive at a group probability and was relied upon to teach this component, in combination with Chirashnya. The same concept of multiplying probabilities to arrive at a group probability is taught in the disclosure of Rogers' provisional application, and as such, the pertinent disclosure of the published application is completely supported in the provisional application, which renders the earlier priority date legitimate. Further, Rogers claims the calculation of a plurality of paths in the publication, which is also discussed in the provisional application.

Claim 21 teaches that a plurality of redundant components is included in the group of non-redundant components. Rogers, in both the provisional and published applications, teaches the concept of redundant components' probabilities (having the same probability) being multiplied together (paragraph 0013 in the published application, and in the fourth equation of page 2 of the provisional application). As such, the pertinent disclosure and concepts thereof of the published application are supported in the provisional application. Please also see the discussion of claim 20.

Regarding claims 22 and 33, as stated earlier, Chirashnya teaches the computing of instantaneous availability. Further, Chirashnya's system is continually updating to reflect the latest network conditions, so instantaneous availability is disclosed.

Claim 39:

Paragraph 0008 in Noy teaches that a network component sends out an identification request to another network component, and the network component sends an identifier back to the network component making the request. As such, Noy teaches the claimed limitation.

The claims of the Noy publication discusses the concepts of service provisioning by request, which is the same subject matter disclosed in the provisional application. As such, Appellant's assertion that the Noy publication and provisional application differ is fallacious. The teaching relied upon in rejecting claim 39, namely the requesting of an identification of a network component, is clearly taught in both the provisional application and the published application.

Motivation to combine teachings lies in the fact that Chirashnya already teaches the service discovery of the network components, by identifying the components discovered, and their related availabilities. The only deficiency in Chirashnya is an explicit request for information for a particular component, and Noy addresses this deficiency. As such motivation to include this teaching into Chirashnya would clearly exist to one of ordinary skill in the art at the time of the invention, to allow for the ability to actively request information about a

particular component for various reasons, including a further monitoring of the component, for example.

Claim 40:

As described above, Chirashnya is replete with examples of teachings of the monitoring of performance of one of the components. Further, Chirashnya teaches an MTBF falling below a certain threshold (0053, 0054, 0063), and if the confidence related to this becomes too high, action is deemed necessary, which constitutes the component failing.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Tanim Hossain

TH

Conferees:

Jason Cardone

Rupal Dharia

JASON CARDONE
SUPERVISORY PATENT EXAMINER

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER